LETTER

# Characterization for a Generic Construction of Bent Functions and Its Consequences

**Yanjun LI**[†,††a)], ***Nonmember***, **Jinjie GAO**[†††,††††b)], **Haibin KAN**[†††,††††,†††††c)], ***Members***, **Jie PENG**[††††††d)], **Lijing ZHENG**[*e)], ***and*** **Changhui CHEN**[*f)], ***Nonmembers***

**SUMMARY** In this letter, we give a characterization for a generic construction of bent functions. This characterization enables us to obtain another efficient construction of bent functions and to give a positive answer on a problem of bent functions.

***key words:*** *bent function, dual, cryptography, Walsh-Hadamard transform*

## 1. Introduction

Bent functions, introduced in [9], are those Boolean functions in an even number of variables having the highest nonlinearity. Such functions have been extensively studied almost five decades, because of their closely relationship with the theory of difference sets, and their significant applications in coding theory and cryptography [3]. In the past, a large amount of work was done on the characterizations and constructions of bent functions. But until now, a complete classification is not finished and it remains elusive. Along with the deep-going of the research, the progress on bent functions becomes more and more difficult, even if a tiny progress is not easy. For a comprehensive book on bent functions, the interested readers are referred to [8] for details.

In this letter, we focus our attention on the characterizations and constructions of bent functions with the form

$$h(x) = f(x) + F \circ \phi(x), \tag{1}$$

where $f$ is a bent function on $\mathbb{F}_{2^n}$, $F$ is a Boolean function on $\mathbb{F}_2^r$, and $\phi = (\phi_1, \phi_2, \ldots, \phi_r)$ is an $(n, r)$-function. In fact, the research on the bent-ness of $h$ can be dated back to [2], where Carlet presented a sufficient condition for a particular case of $h$ to be bent. That sufficient condition had been proved by Mesnager [7] to be necessary. Mesnager [7] also studied the bent-ness of two particular cases of Carlet function, from which Mesnager obtained a lot of bent functions and gave their duals. Thereafter, several papers (such as [5], [10], [11], [12], [13]) were done for generalizing Carlet's and Mesnager's works.

In this letter, we obtain a characterization for the generic construction of bent functions given in [5], which enables us to find another efficient construction of bent functions. This characterization also enables us to provide a positive answer on the problem of bent function proposed in Conclusion of [5].

## 2. Preliminaries

Throughout the paper, let $n = 2m$ be an even positive integer. Let $\mathbb{F}_{2^n}$ be the finite field of order $2^n$, $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$, and $\mathbb{F}_2^n$ be the $n$-dimensional vector space over $\mathbb{F}_2$.

For a vector $\omega = (\omega_1, \omega_2, \ldots, \omega_n) \in \mathbb{F}_2^n$, the set $\mathrm{suppt}(\omega) = \{1 \le i \le n : \omega_i \ne 0\}$ is said to be the *support* of $\omega$, whose cardinality is called the *(Hamming) weight* of $\omega$, denoted by $wt(\omega)$. Namely, $wt(\omega) = |\mathrm{suppt}(\omega)|$.

A mapping $\phi$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2^r$ is called an *$(n, r)$-function*. When $n$ is divisible by $r$, the $(n, r)$-function

$$\mathrm{Tr}_r^n(x) = x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{n-r}}$$

is called the *trace function*. The set of all $(n, 1)$-functions (namely, all *Boolean functions*) is denoted by $\mathcal{B}_n$.

For a given Boolean function $f$ on $\mathbb{F}_2^n$, the *Walsh-Hadamard transform* of $f$ is a mapping from $\mathbb{F}_2^n$ to $\mathbb{Z}$ defined as

$$W_f(\mu) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \mu \cdot x}, \quad \mu \in \mathbb{F}_2^n,$$

and its *inverse transform* is given by

$$(-1)^{f(\mu)} = 2^{-n} \sum_{x \in \mathbb{F}_2^n} W_f(x)(-1)^{\mu \cdot x}, \quad \mu \in \mathbb{F}_2^n,$$

where $\mu \cdot x$ denotes the canonical inner product of $\mu$ and $x$

Manuscript received March 11, 2024.
Manuscript publicized May 7, 2024.

[†]Institute of Statistics and Applied Mathematics, Anhui University of Finance and Economics, Bengbu, Anhui 233030, China.
[††]School of Computer Sciences, Fudan University, Shanghai, 200433, China.
[†††]Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai 200433, China.
[††††]Shanghai Engineering Research Center of Blockchain, Shanghai 200433, China.
[†††††]Yiwu Research Institute of Fudan University, Yiwu City 322000, China.
[††††††]Mathematics and Science College of Shanghai Normal University, Guilin Road #100, Shanghai 200234, China.
[*]School of Mathematics and Physics, University of South China, Hengyang, Hunan 421001, China.
a) E-mail: yanjlmath90@163.com
b) E-mail: jjgao18@fudan.edu.cn
c) E-mail: hbkan@fudan.edu.cn
d) E-mail: jpeng@shnu.edu.cn
e) E-mail: zhenglijing817@163.com
f) E-mail: cchxuexi@126.com

DOI: 10.1587/transfun.2024EAL2032

(in $\mathbb{F}_{2^n}$, $\mu \cdot x = \mathrm{Tr}_1^n(\mu x)$).

The *first derivative* of $f$ in terms of $\mu \in \mathbb{F}_2^n$ is defined as

$$D_\mu f(x) = f(x) + f(x+\mu),$$

and the *second derivative* of $f$ with $\mu, \nu \in \mathbb{F}_2^n$ is defined as

$$D_\mu D_\nu f(x) = f(x) + f(x+\mu) + f(x+\nu) + f(x+\mu+\nu).$$

**Definition 1.** *A Boolean function $f$ on $\mathbb{F}_2^n$ is called bent if $n$ is even and $W_f(\mu) = \pm 2^{\frac{n}{2}}$ for all $\mu \in \mathbb{F}_2^n$.*

Bent functions always appear in pairs, that is, for any bent function $f$ on $\mathbb{F}_2^n$, there is always a unique bent function $f^*$ such that $W_f(\mu) = 2^{\frac{n}{2}}(-1)^{f^*(\mu)}$ for all $\mu \in \mathbb{F}_2^n$ (in literatures, $f^*$ is called the *dual* of $f$).

## 3. A Characterization of a Generic Construction of Bent Functions

In [5], the authors have given a generic construction of bent functions, which generalizes the constructions of bent functions given in [2], [7], [10], [11], [12], [13]. We restate it as follows.

**Theorem 1.** *[5, Theorem 3] Let $i$ be an integer with $1 \le i \le r$, $f, g_i \in \mathcal{B}_n$, and let $\phi = (\phi_1, \phi_2, \ldots, \phi_r)$ be the $(n,r)$-function with $\phi_i = f + g_i$. If the sum of any odd number of functions in $f, g_1, \ldots, g_r$ is a bent function, and its dual is equal to the sum of the duals of corresponding bent functions. Then for any Boolean function $F$ on $\mathbb{F}_2^r$, the function $h$ given by* (1) *is bent, and the dual of $h$ is*

$$h^*(x) = f^*(x) + F \circ \varphi(x),$$

*where $\varphi = (\varphi_1, \varphi_2, \ldots, \varphi_r)$ is the $(n,r)$-function with $\varphi_i(x) = f^*(x) + g_i^*(x)$, $1 \le i \le r$.*

Below, we want to generalize Theorem 1 by using the following property.

**Definition 2 ($\mathbf{P_r}$).** *Let $f$ be a Boolean function over $\mathbb{F}_{2^n}$. If there is an $(n,r)$-function $\phi = (\phi_1, \phi_2, \ldots, \phi_r)$ such that the following two conditions are satisfied:*

*(i) $f(x) + \omega \cdot \phi(x) = f(x) + \sum_{i=1}^r \omega_i \phi_i$ is bent for any $\omega = (\omega_1, \omega_2, \ldots, \omega_r) \in \mathbb{F}_2^r$;*

*(ii) there is an $(n,r)$-function $\varphi = (\varphi_1, \varphi_2, \ldots, \varphi_r)$ such that $\big(f(x) + \omega \cdot \phi(x)\big)^* = f^*(x) + \omega \cdot \varphi(x)$ for any $\omega \in \mathbb{F}_2^r$,*

*then we say that $f$ satisfies $\mathbf{P_r}$ with respect to the $(n,r)$-function $\phi$.*

**Theorem 2.** *Let $n = 2m$. Let $\phi$ be an $(n,r)$-function, and let $f$ be a Boolean function on $\mathbb{F}_{2^n}$ satisfying $\mathbf{P_r}$ with respect to $\phi$. Then for any Boolean function $F$ on $\mathbb{F}_2^r$, the function $h$ given by* (1) *is bent, and the dual of $h$ is*

$$h^*(x) = f^*(x) + F \circ \varphi(x).$$

*Proof.* By the definition of the inverse Walsh-Hadamard transform, it holds that

$$(-1)^{F\circ\phi(x)} = 2^{-r} \sum_{\omega \in \mathbb{F}_2^r} W_F(\omega)(-1)^{\omega\cdot\phi(x)}, \ \ \forall\, x \in \mathbb{F}_2^n.$$

Hence, the Walsh-Hadamard transform of $h$ at $\beta \in \mathbb{F}_{2^n}$ is that

$$\begin{aligned} W_h(\beta) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(\beta x)}(-1)^{F\circ\phi(x)} \\ &= 2^{-r} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(\beta x)} \sum_{\omega\in\mathbb{F}_2^r} W_F(\omega)(-1)^{\omega\cdot\phi(x)} \\ &= 2^{-r} \sum_{\omega\in\mathbb{F}_2^r} W_F(\omega) \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(\beta x)+\omega\cdot\phi(x)} \\ &= 2^{-r} \sum_{\omega\in\mathbb{F}_2^r} W_F(\omega) W_g(\beta), \end{aligned}$$

where $g(x) = f(x) + \omega \cdot \phi(x)$. Recall that $f$ satisfies $\mathbf{P_r}$ with respect to $\phi$, that is, $g$ is bent and $g^*(x) = f^*(x) + \omega \cdot \varphi(x)$ for any $\omega \in \mathbb{F}_2^r$. Hence, we have

$$\begin{aligned} W_h(\beta) =& 2^{m-r} \sum_{\omega\in\mathbb{F}_2^r} W_F(\omega)(-1)^{f^*(\beta)+\omega\cdot\varphi(\beta)} \\ =& 2^m (-1)^{f^*(\beta)+F\circ\varphi(\beta)}. \end{aligned}$$

The proof is completed. □

**Corollary 1.** *Theorem 2 is reduced to that of Theorem 1 when $\phi = (\phi_1, \phi_2, \ldots, \phi_r)$ is an $(n,r)$-function with $\phi_i = f + g_i$, $1 \le i \le r$, where $f$ and $g_i$ are any Boolean functions on $\mathbb{F}_{2^n}$.*

*Proof.* Suppose that $\phi = (\phi_1, \phi_2, \ldots, \phi_r)$ with $\phi_i = f + g_i$, $1 \le i \le r$. Then for any $\omega = (\omega_1, \omega_2, \ldots, \omega_r) \in \mathbb{F}_2^r$, we have

$$\begin{aligned} f(x) + \omega\cdot\phi(x) &= f(x) + \sum_{i=1}^r \omega_i (f(x) + g_i(x)) \\ &= \begin{cases} G_\omega(x), & \text{if } wt(\omega) \text{ is odd,} \\ f(x) + G_\omega(x), & \text{if } wt(\omega) \text{ is even,} \end{cases} \end{aligned}$$

where $G_\omega(x) = \omega_1 g_1(x) + \omega_2 g_2(x) + \cdots + \omega_r g_r(x)$. Therefore, Item (i) of $\mathbf{P_r}$ holds if and only if the sum of any odd number of functions in $f, g_1, g_2, \ldots, g_r$ is bent. When $\mathrm{suppt}(\omega) = \{i\}$, we have

$$f(x) + \omega\cdot\phi(x) = g_i(x), f^*(x) + \omega\cdot\varphi(x) = f^*(x) + \varphi_i(x).$$

So Item (ii) of $\mathbf{P_r}$ holds only if $\varphi_i(x) = f^*(x) + g_i^*(x)$ for any integer $i$, $1 \le i \le r$. In this case,

$$\begin{aligned} f^*(x) + \omega\cdot\varphi(x) &= f^*(x) + \sum_{i=1}^r \omega_i (f^*(x) + g_i^*(x)) \\ &= \begin{cases} G_\omega^*(x), & \text{if } wt(\omega) \text{ is odd,} \\ f^*(x) + G_\omega^*(x), & \text{if } wt(\omega) \text{ is even,} \end{cases} \end{aligned}$$

where $G^*_\omega(x) = \omega_1 g^*_1(x) + \omega_2 g^*_2(x) + \cdots + \omega_r g^*_r(x)$. Hence, Item (ii) of $\mathbf{P_r}$ holds if and only if $(G_\omega)^* = G^*_\omega$ when $wt(\omega)$ is odd, and $(f + G_\omega)^* = f^* + G^*_\omega$ when $wt(\omega)$ is even. Equivalently, the dual of the sum of any odd number of functions in $f, g_1, g_2, \ldots, g_r$ is equal to the sum of the duals of corresponding bent functions. This completes the proof. □

From the proof of Corollary 1, it is easily seen that for a given Boolean function $f$ on $\mathbb{F}_{2^n}$, and an $(n,r)$-function $\phi = (\phi_1, \phi_2, \ldots, \phi_r)$, $\mathbf{P_r}$ holds if and only if the sum of any odd number of functions in $f, f + \phi_1, f + \phi_2, \ldots, f + \phi_r$ is bent, and its dual is equal to the sum of the duals of corresponding bent functions. Namely, Theorem 1 is another characterization of Theorem 2. Note that Theorem 1 was proved by induction in [5]. Here we provide a more simple alternative proof from another perspective.

Theorem 2 allows us to deduce the following result.

**Corollary 2.** *Let $n = 2m$. Let $f$ and $g$ be two bent functions on $\mathbb{F}_{2^n}$. Let $\mu_2, \mu_3, \ldots, \mu_r \in \mathbb{F}^*_{2^n}$. If the following two conditions are satisfied:*

*(A) $D_{\mu_i} D_{\mu_j} f^* = 0$ for any $2 \le i < j \le r$;*

*(B) for any $\omega' = (\omega_2, \omega_3, \ldots, \omega_r) \in \mathbb{F}_2^{r-1}$, it holds that*

$$g^*(x + \sum_{i=2}^{r} \omega_i \mu_i) = \begin{cases} g^*(x) + f^*(x) + \sum_{i=2}^{r} \omega_i f^*(x + \mu_i), & \text{if } wt(\omega') \text{ is odd}, \\ g^*(x) + \sum_{i=2}^{r} \omega_i f^*(x + \mu_i), & \text{if } wt(\omega') \text{ is even}, \end{cases} \quad (2)$$

*then for any Boolean function $F$ on $\mathbb{F}_2^r$, the function $h$ given by*

$$h(x) = f(x) + F(f(x) + g(x), \mathrm{Tr}_1^n(\mu_2 x), \ldots, \mathrm{Tr}_1^n(\mu_r x))$$

*is bent. Moreover, the dual of $h$ is*

$$h^*(x) = f^*(x) + F(\varphi_1, \varphi_2, \ldots, \varphi_r),$$

*where $\varphi_1(x) = f^*(x) + g^*(x)$ and $\varphi_i(x) = f^*(x) + f^*(x + \mu_i)$ for any integer $2 \le i \le r$.*

*Proof.* Let $\phi = (\phi_1, \phi_2, \ldots, \phi_r)$ be the $(n,r)$-function with $\phi_1(x) = f(x) + g(x)$ and $\phi_i(x) = \mathrm{Tr}_1^n(\mu_i x)$ for each $2 \le i \le r$. Then for any $\omega = (\omega_1, \omega_2, \ldots, \omega_r) \in \mathbb{F}_2^r$, it is easily seen that

$$f(x) + \omega \cdot \phi(x) = \begin{cases} f(x) + \mathrm{Tr}_1^n((\omega_2\mu_2 + \cdots + \omega_r\mu_r)x), & \text{if } \omega_1 = 0, \\ g(x) + \mathrm{Tr}_1^n((\omega_2\mu_2 + \cdots + \omega_r\mu_r)x), & \text{if } \omega_1 = 1. \end{cases}$$

This implies that Item (i) of $\mathbf{P_r}$ is satisfied when $f$ and $g$ are bent. So we have

$$\big(f(x) + \omega \cdot \phi(x)\big)^* = \begin{cases} f^*(x + \omega_2\mu_2 + \cdots + \omega_r\mu_r), & \text{if } \omega_1 = 0, \\ g^*(x + \omega_2\mu_2 + \cdots + \omega_r\mu_r), & \text{if } \omega_1 = 1. \end{cases}$$

Note that when $\mathrm{suppt}(\omega) = \{i\}$, we have

$$f(x) + \omega \cdot \phi(x) = \begin{cases} g(x), & \text{if } i = 1, \\ f(x) + \mathrm{Tr}_1^n(\mu_i x) & \text{otherwise}, \end{cases}$$

and $f^*(x) + \omega \cdot \varphi(x) = f^*(x) + \varphi_i(x)$. Hence, Item (ii) of $\mathbf{P_r}$ holds only if $\varphi_1(x) = f^*(x) + g^*(x)$ and $\varphi_i(x) = f^*(x) + f^*(x + \mu_i)$ for any $2 \le i \le r$. In this case,

$$f^*(x) + \omega \cdot \varphi(x) = \begin{cases} f^*(x) + \sum_{i=2}^{r} \omega_i (f^*(x) + f^*(x + \mu_i)), & \text{if } \omega_1 = 0, \\ g^*(x) + \sum_{i=2}^{r} \omega_i (f^*(x) + f^*(x + \mu_i)), & \text{if } \omega_1 = 1. \end{cases}$$

Hence, Item (ii) of $\mathbf{P_r}$ holds if and only if the following two relations hold:

$$\begin{aligned} & f^*(x + \omega_2\mu_2 + \cdots + \omega_r\mu_r) \\ =& f^*(x) + \sum_{i=2}^{r} \omega_i (f^*(x) + f^*(x + \mu_i)) \\ =& \begin{cases} f^*(x) + \sum_{i=2}^{r} \omega_i f^*(x + \mu_i), & \text{if } wt(\omega') \text{ is even}, \\ \sum_{i=2}^{r} \omega_i f^*(x + \mu_i), & \text{if } wt(\omega') \text{ is odd}, \end{cases} \end{aligned} \quad (3)$$

and

$$\begin{aligned} & g^*(x + \omega_2\mu_2 + \cdots + \omega_r\mu_r) \\ =& g^*(x) + \sum_{i=2}^{r} \omega_i (f^*(x) + f^*(x + \mu_i)) \\ =& \begin{cases} g^*(x) + \sum_{i=2}^{r} \omega_i f^*(x + \mu_i), & \text{if } wt(\omega') \text{ is even}, \\ g^*(x) + f^*(x) + \sum_{i=2}^{r} \omega_i f^*(x + \mu_i), & \text{if } wt(\omega') \text{ is odd}, \end{cases} \end{aligned} \quad (4)$$

where $\omega' = (\omega_2, \omega_3, \ldots, \omega_r)$. By [13, Lemma 3.3], we know that Relation (3) holds if and only if $D_{\mu_i} D_{\mu_j} f^* = 0$ for any $2 \le i < j \le r$. Then the result follows from Theorem 2 immediately. □

Note that Condition (B) of Corollary 2 is elusive when $r > 2$. In the following corollary, we give a reduced form by applying Corollary 2 to $g(x) = f(x + \alpha)$ for some $\alpha \in \mathbb{F}^*_{2^n}$.

**Corollary 3.** *Let $f$ be a bent function on $\mathbb{F}_{2^n}$. Let $\alpha \in \mathbb{F}_{2^n}$ and $\mu_2, \mu_3, \ldots, \mu_r \in \mathbb{F}^*_{2^n}$ be such that $\alpha \in \langle \mu_2, \mu_3, \ldots, \mu_r \rangle^\perp$ and $D_{\mu_i} D_{\mu_j} f^* = 0$ for any $2 \le i < j \le r$. Then for any Boolean function $F$ on $\mathbb{F}_2^r$, the function*

$$h(x) = f(x) + F(f(x) + f(x + \alpha), \mathrm{Tr}_1^n(\mu_2 x), \ldots, \mathrm{Tr}_1^n(\mu_r x))$$

*is bent. Moreover, the dual of $h$ is*

$$h^*(x) = f^*(x) + F(\varphi_1, \varphi_2, \ldots, \varphi_r),$$

*where $\varphi_1(x) = \mathrm{Tr}_1^n(\alpha x)$ and $\varphi_i(x) = f^*(x) + f^*(x + \mu_i)$ for any integer $2 \le i \le r$.*

*Proof.* Let $g(x) = f(x+\alpha)$. Then it is easily seen that $g^*(x) = f^*(x) + \mathrm{Tr}_1^n(\alpha x)$, and then Relation (2) becomes that

$$f^*(x + \sum_{i=2}^{r} \omega_i \mu_i) = \begin{cases} \sum_{i=2}^{r} \omega_i f^*(x+\mu_i), & \text{if } wt(\omega') \text{ is odd}, \\ f^*(x) + \sum_{i=2}^{r} \omega_i f^*(x+\mu_i), & \text{if } wt(\omega') \text{ is even}, \end{cases}$$

since $\alpha \in \langle \mu_2, \mu_3, \ldots, \mu_r \rangle^\perp$. Hence, Condition (B) of Corollary 2 is satisfied if and only if $D_{\mu_i} D_{\mu_j} f^* = 0$ for any $2 \le i < j \le r$ by [13, Lemma 3.3]. Then the result follows from Corollary 2 directly. □

**Remark 1.** *Note that though the conditions of h to be bent in Corollary 3 are similar as that of given in [13, Theorem 3.5] (in fact, Corollary 3 is reduced to [13, Theorem 3.5] when* $\alpha = 0$*), the corresponding bent functions in Corollary 3 and [13, Theorem 3.5] can be EA-inequivalent. For instance, let* $n = 6$ *and*

$$f(x) = (x_1, x_2, x_3) \cdot (x_4, x_5, x_6).$$

*Let* $\mu_2 = (1,0,0,0,0,0)$, $\mu_3 = (0,1,1,0,0,0)$. *Then it is easy to check that* $D_{\mu_2} D_{\mu_3} f^* = 0$. *Hence, by [13, Theorem 3.5], we have that*

$$h(x) = f(x) + F(\mu_2 \cdot x, \mu_3 \cdot x) = f(x) + F(x_1, x_2 + x_3)$$

*is bent for any Boolean function F on* $\mathbb{F}_2^2$*; and by Corollary 3, we have that*

$$\begin{aligned} \hat{h}(x) &= f(x) + \hat{F}\big(f(x) + f(x+\alpha), \mu_2 \cdot x, \mu_3 \cdot x\big) \\ &= f(x) + \hat{F}\big(f(x) + f(x+\alpha), x_1, x_2 + x_3\big) \end{aligned}$$

*is bent for any* $\alpha \in \langle \mu_2, \mu_3 \rangle^\perp$ *and any Boolean function* $\hat{F}$ *on* $\mathbb{F}_2^3$. *These two bent functions can be clearly EA-inequivalent, since the algebraic degree of h is 2, while the algebraic degree of* $\hat{h}$ *is 3 when* $\alpha = \mu_3$ *and* $\hat{F}(x_1, x_2, x_3) = x_1 x_2 x_3$.

In [5], the authors have found two kinds of $f$ and $\phi$ satisfying the conditions of Theorem 1 (that is, $\mathbf{P_r}$ by the previous discussion) for constructing new bent functions. The first kind is to let $f$ be a bent function and $\phi$ be a linear $(n,r)$-function; and the second kind is to let $f$ and $f + \phi_i$ be some self-dual bent functions for each $1 \le i \le r$. They also invited the readers to find more kinds of $f$ and $\phi$ for obtaining more classes of bent functions in Conclusion of [5]. Note that we have found a method to find such kinds of $f$ and $\phi$ in Corollary 3.

Then similarly as the concrete bent functions obtained in [5], [11], [12] and [13], by applying Corollary 3 to the following three monomial bent functions

$$f_1(x) = \mathrm{Tr}_1^n(\lambda x^{2^t+1}),$$
$$f_2(x) = \mathrm{Tr}_1^{6k}(\lambda x^{2^{2k}+2^k+1}),$$
$$f_3(x) = \mathrm{Tr}_1^{4k}(\lambda x^{2^{2k}+2^{k+1}+1}),$$

respectively; and to the following bent functions with Niho exponents

$$f_4(x) = \mathrm{Tr}_1^m(x^{2^m+1}) + \mathrm{Tr}_1^n\Big(\sum_{i=1}^{2^{k-1}-1} x^{(2^m-1)\frac{i}{2^k}+1}\Big),$$

one can also obtain certain concrete bent functions, since by Corollary 3, one only needs to determine the duals of $f_1, f_2, f_3, f_4$ (which have been done in [4], [5], [6] and [1], respectively), find some elements $\mu_2, \mu_3, \ldots, \mu_r \in \mathbb{F}_{2^n}^*$ such that $D_{\mu_i} D_{\mu_j} f_e^* = 0$ for any $2 \le i < j \le r$ and any $1 \le e \le 4$ (such elements exist by [7], [10], [11], [12], [13]), and find some $\alpha \in \mathbb{F}_{2^n}$ such that $\alpha \in \langle \mu_2, \mu_3, \ldots, \mu_r \rangle^\perp$. Here, the concrete results do not unfolded in details.

## 4. Conclusion

This paper gave another characterization for the generic construction of bent functions given in [5], which enabled us to obtain another efficient construction of bent functions and to provide a positive answer on the problem of bent functions proposed in Conclusion of [5].


## Acknowledgments

This work was supported in part by the National Key Research and Development Program of China under Grant 2019YFB2101703, in part by the National Natural Science Foundation of China under Grants 62302001, 62372221, 61972258 and 62272107, in part by the China Postdoctoral Science Foundation under Grant 2023M740714, in part by the Innovation Action Plan of Shanghai Science and Technology under Grant 21511102200, in part by the Key Research and Development Program of Guangdong Province under Grant 2020B0101090001, in part by the Natural Science Foundation for the Higher Education Institutions of Anhui Province under Grant 2023AH050250.


### References


[1] L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager, "Further results on Niho bent functions," IEEE Trans. Inf. Theory, vol.58, no.11, pp.6979–6985, 2012.

[2] C. Carlet, "On bent and highly nonlinear balanced/resilient functions and their algebraic immunities," Proc. AAECC, vol.3857, pp.1–28, Springer, Berlin, Germany 2006.

[3] C. Carlet, Boolean Functions for Cryptography and Coding Theory, Cambridge University Press, Cambridge, 2021.

[4] N.G. Leander, "Monomial bent functions," IEEE Trans. Inf. Theory, vol.52, no.2, pp.738–743, 2006.

[5] Y. Li, H. Kan, S. Mesnager, J. Peng, C.H. Tan, and L. Zheng, "Generic constructions of (Boolean and vectorial) bent functions and their consequences," IEEE Trans. Inf. Theory, vol.68, no.4, pp.2735–2751, 2022.

[6] Y. Li, H. Kan, J. Peng, C.H. Tan, and B. Liu, "The explicit dual of Leander's monomial bent function," IEICE Trans. Fundamentals, vol.E104-A, no.9, pp.1357–1360, 2021.

[7] S. Mesnager, "Several new infinite families of bent functions and their duals," IEEE Trans. Inf. Theory, vol.60, no.7, pp.4397–4407, 2014.

[8] S. Mesnager, Bent Functions: Fundamentals and Results, Springer, Cham, Switzerland, 2016.
[9] O. Rothaus, "On "bent" functions," J. Combin. Theory Ser. A, vol.20, no.3, pp.300–305, 1976.
[10] C. Tang, Z. Zhou, Y. Qi, X. Zhang, C. Fan, and T. Helleseth, "Generic construction of bent functions and bent idempotents with any possible algebraic degrees," IEEE Trans. Inf. Theory, vol.63, no.10, pp.6149–6157, 2017.
[11] L. Wang, B. Wu, Z. Liu, and D. Lin, "Three new infinite families of bent functions," Sci. China Inf. Sci., vol.61, no.3, p.032104, 2018.
[12] G. Xu, X. Cao, and S. Xu, "Several new classes of Boolean functions with few Walsh transform values, Appl. Algebra Eng. Commun. Comput., vol.28, no.2, pp.155–176, 2017.
[13] L. Zheng, J. Peng, H. Kan, and Y. Li, "Several new infinite families of bent functions via second order derivatives," Cryptogr. Commun., vol.12, no.6, pp.1143–1160, 2020.